

Załącznik nr 1 do Umowy Umowa powierzenia przetwarzania danych osobowych nr  ……………….. z dnia………………….

**Wykaz stosowanych środków**

**Ankieta dla Podmiotu przetwarzającego**

**…………………………………………………** *(nazwa Podmiotu przetwarzającego)*, stosuje właściwe środki organizacyjne i techniczne umożliwiające należyte zabezpieczenie danych osobowych, zgodnie z RODO (Rozporządzenie 2016/679)

1. Została opracowana i wdrożona dokumentacja w zakresie ochrony danych osobowych

*(poniżej należy wymienić kluczową opracowaną i wdrożoną dokumentację):*

obowiązują odpowiednie regulacje wewnętrzne m.in. Polityka i instrukcja ochrony danych oraz System Zarządzania Bezpieczeństwem Informacji oraz System Zarządzania Ciągłością Działania;

prowadzony jest rejestr czynności przetwarzania danych osobowych i rejestr kategorii czynności przetwarzania zgodnie z art. 30 RODO;

obowiązują procedury dotyczące:

* zarządzania incydentami bezpieczeństwa i naruszeń danych osobowych,
* klasyfikacji informacji,
* realizacji żądań/praw podmiotów danych,
* realizacji obowiązku informacyjnego,

2. Wdrożono środki organizacyjne ochrony danych osobowych:

*(poniżej należy wymienić kluczowe środki organizacyjne)*

funkcjonuje jednostka odpowiedzialna za ochronę danych osobowych - Inspektor Ochrony Danych;

pracownicy posiadają upoważnienia do przetwarzania danych osobowych, oraz podpisane oświadczenia o zachowaniu poufności;

pracownicy odbywają systematyczne szkolenia w zakresie ochrony danych osobowych oraz   
z zakresu bezpieczeństwa informacji;

pracownicy zobowiązani są do przestrzegania zasad i opisanych w dokumentach wewnętrznych w zakresie bezpieczeństwa informacji i ochrony danych osobowych (m.in. polityka „czystego biurka”, „czystego ekranu”, klasyfikacja informacji);

funkcjonuje dedykowana komórka zajmująca się obszarem bezpieczeństwa   
w odniesieniu do procesów realizowanych przez Beneficjenta;

obowiązują zasady dotyczące m.in.: kontroli dostępu, współpracy ze stronami trzecimi, bezpieczeństwa fizyczno-środowiskowego, bezpieczeństwa teleinformatycznego;

regulacje wewnętrzne podlegają systematycznym przeglądom w celu zapewnienia ich aktualności i przydatności.

3. Wdrożono środki ochrony fizycznej i technicznej danych osobowych:

*(poniżej należy wymienić kluczowe środki fizyczne i techniczne)*

Beneficjent posiada wdrożone odpowiednie środki techniczne w obszarze bezpieczeństwa IT;

dostęp do systemu możliwy jest tylko dla uprawnionych użytkowników. System wymaga uwierzytelnienia użytkownika;

dostęp do danych jest kontrolowany uprawnieniami użytkownika;

Beneficjent posiada wdrożone odpowiednie środki techniczne w obszarze bezpieczeństwa IT (m.in. system antywirusowy, system antyspamowy; system do konsolidowania, korelowania, oceny i priorytetyzacji zdarzeń dotyczących bezpieczeństwa IT, systemy d wykrywania   
i zapobiegania włamaniom);

Beneficjent posiada wdrożone odpowiednie środki techniczne w obszarze bezpieczeństwa fizyczno-środowiskowego (BMS, SKD, SSWiN, CCTV);

Beneficjent cyklicznie prowadzi badania podatności środowiska sieciowego oraz przeprowadza testy bezpieczeństwa;

Beneficjent monitoruje źródła informacji zewnętrznej w poszukiwaniu zagrożeń bezpieczeństwa;

Beneficjent w ramach obszaru BCM cyklicznie realizuje testy ciągłości działania w celu ciągłości realizacji poszczególnych procesów;

Beneficjent posiada wydzielone obszary, w których przetwarza się informacje krytyczne lub poufne, granicami o odpowiednich barierach dostępu fizycznego;

Przydzielanie praw dostępu (oraz zarządzanie nimi i nadzór) odbywa się w sposób formalny,   
z uwzględnieniem zasady „minimalnych uprawnień” oraz z uwzględnieniem zakresu obowiązków;

obowiązują zasady ochrony urządzeń przenośnych zarówno w kontekście bezpieczeństwa fizyczno- środowiskowego jak i bezpieczeństwa teleinformatycznego,

Informacje dotyczące danych osobowych nie mogą być przekazywane w formie niezaszyfrowanej;

obowiązują zasady dotyczące wykonywania kopii zapasowych.

…………………………………………………………………………………….

Podpis Podmiotu przetwarzającego